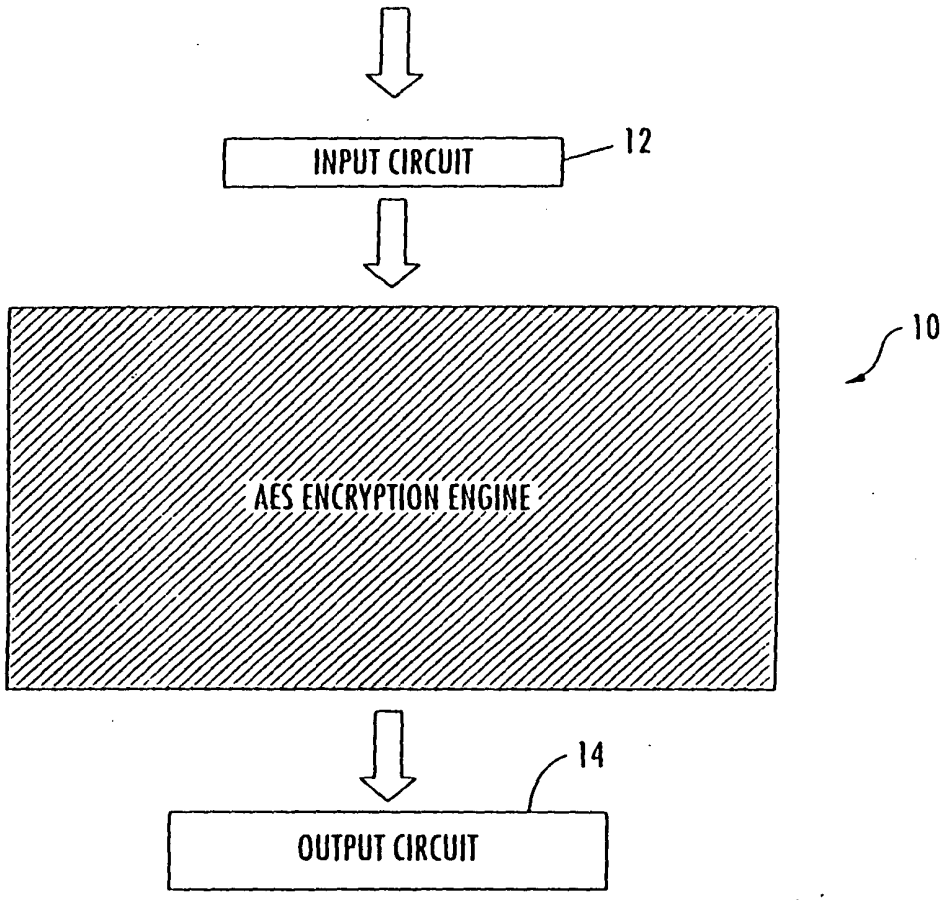

INPUT CIRCUIT
12
AES ENCRYPTION ENGINE
10
14
OUTPUT CIRCUIT

FIG. 1.

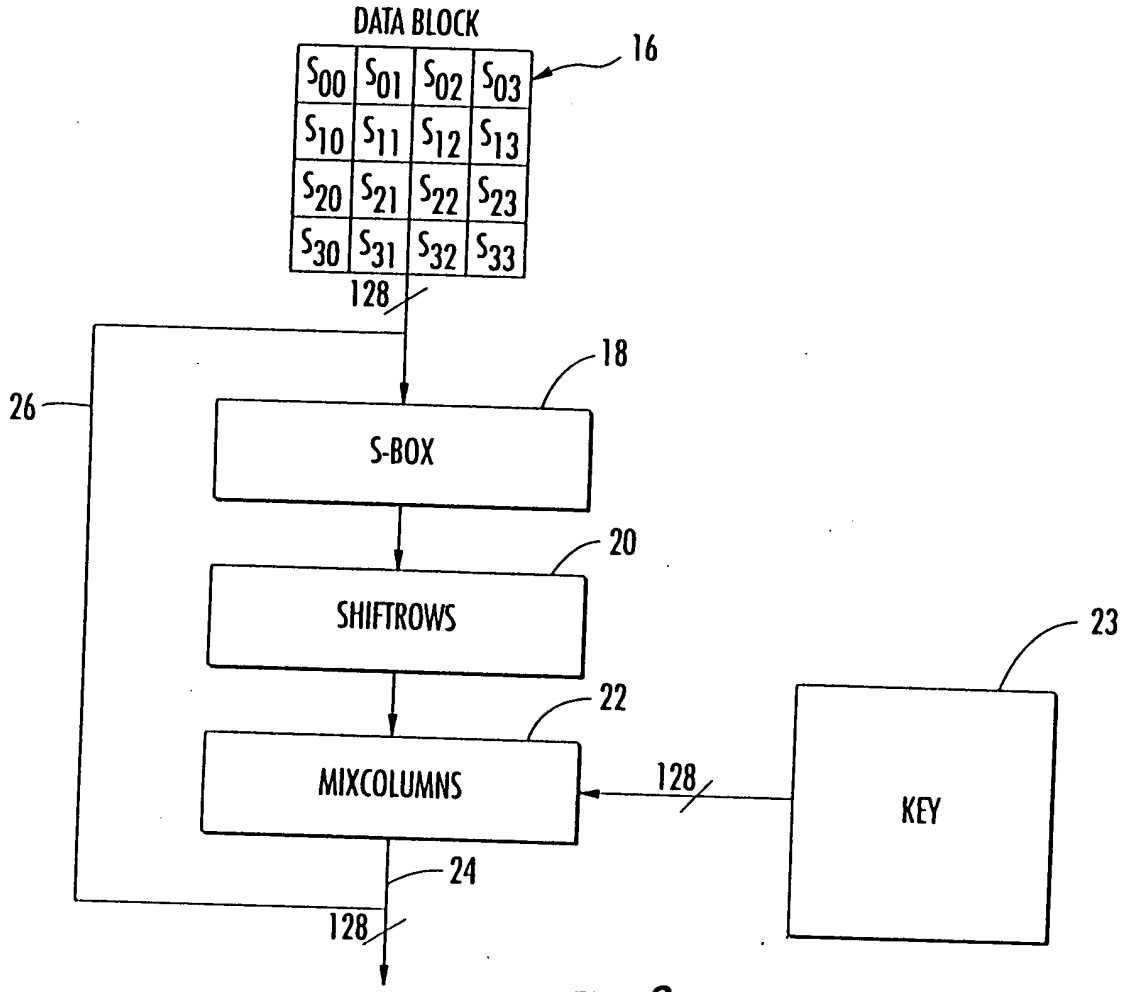

DATA BLOCK
16
S_{00} S_{01} S_{02} S_{03}
S_{10} S_{11} S_{12} S_{13}
S_{20} S_{21} S_{22} S_{23}
S_{30} S_{31} S_{32} S_{33}
128
18
26
S-BOX
20
SHIFTROWS
23
22
MIXCOLUMNS
128
KEY
24
128

FIG. 2.

FIG. 3.

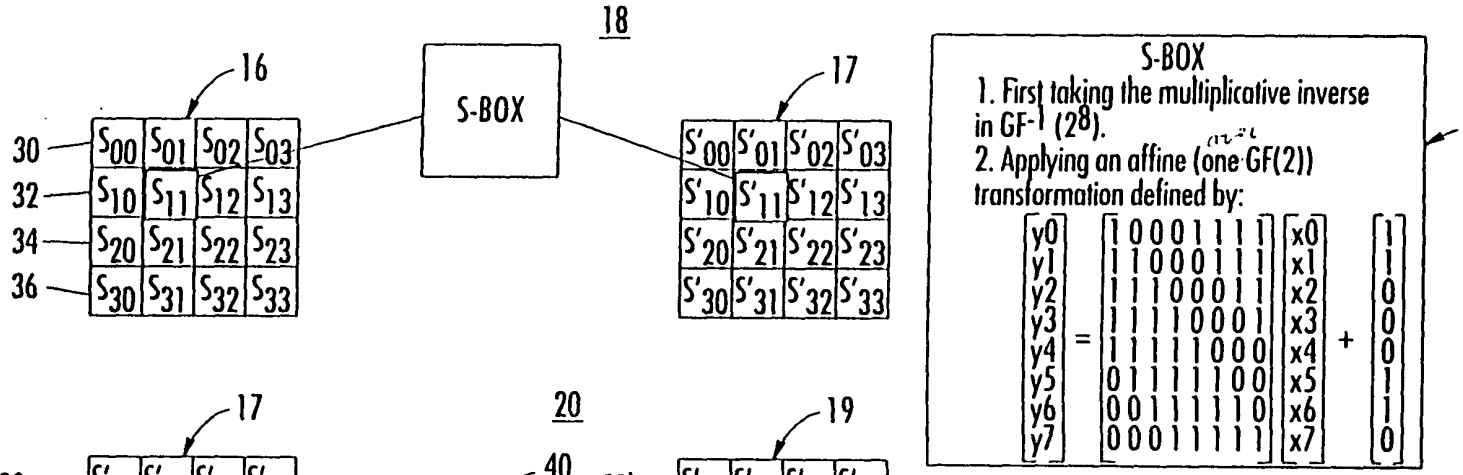


FIG. 4.

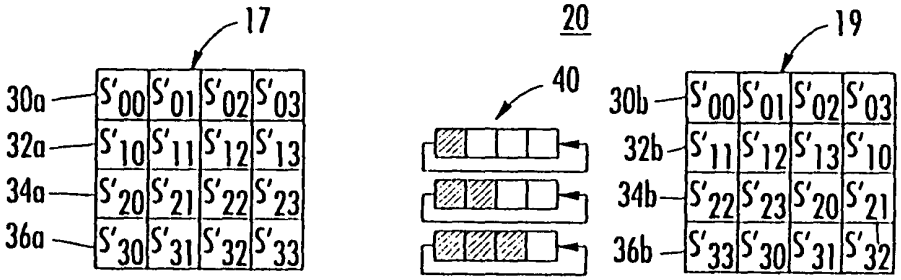
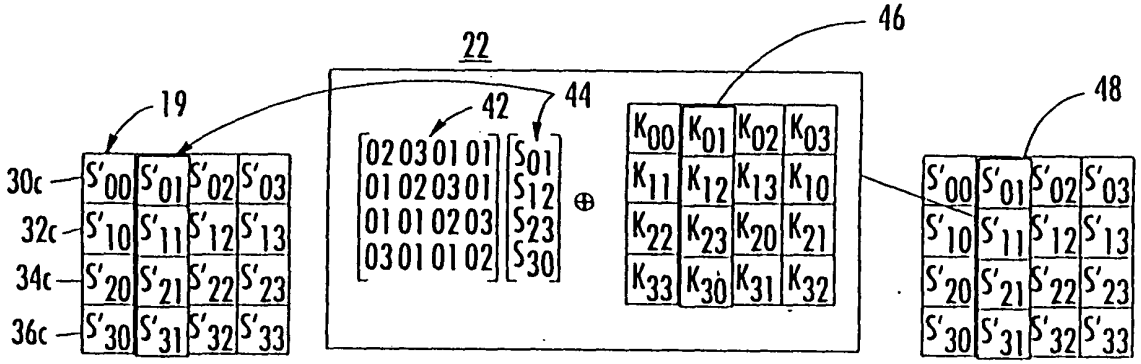


FIG. 5.



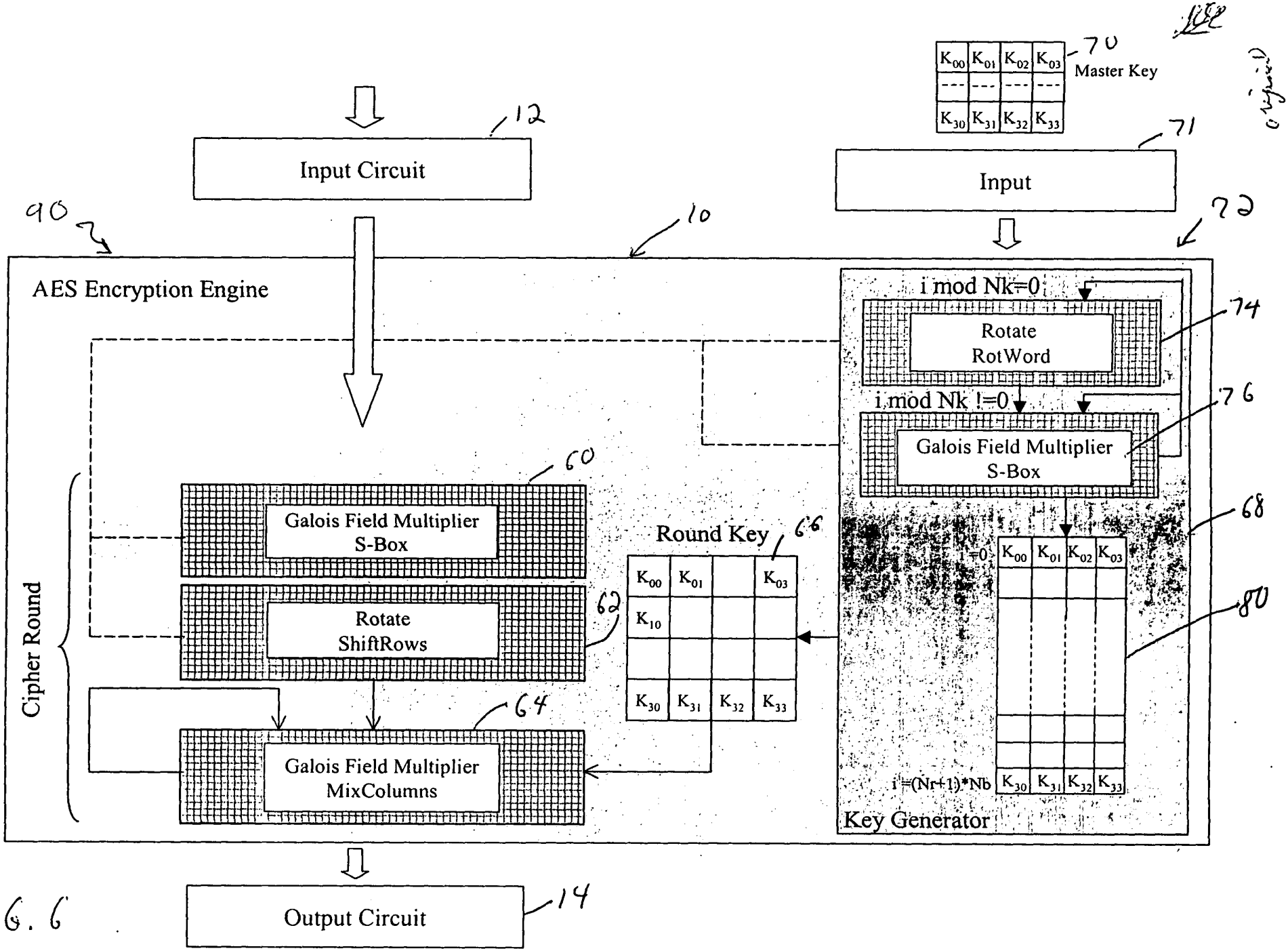

Input Circuit
12
Input
71
Master Key
70
90
10
72
AES Encryption Engine
i mod Nk=0
Rotate
RotWord
74
i mod Nk !=0
Galois Field Multiplier
S-Box
76
60
Galois Field Multiplier
S-Box
Round Key
66
68
Cipher Round
Rotate
ShiftRows
62
i=0
80
64
Galois Field Multiplier
MixColumns
i=(Nr+1)*Nb
Key Generator
Output Circuit
14

FIG. 6

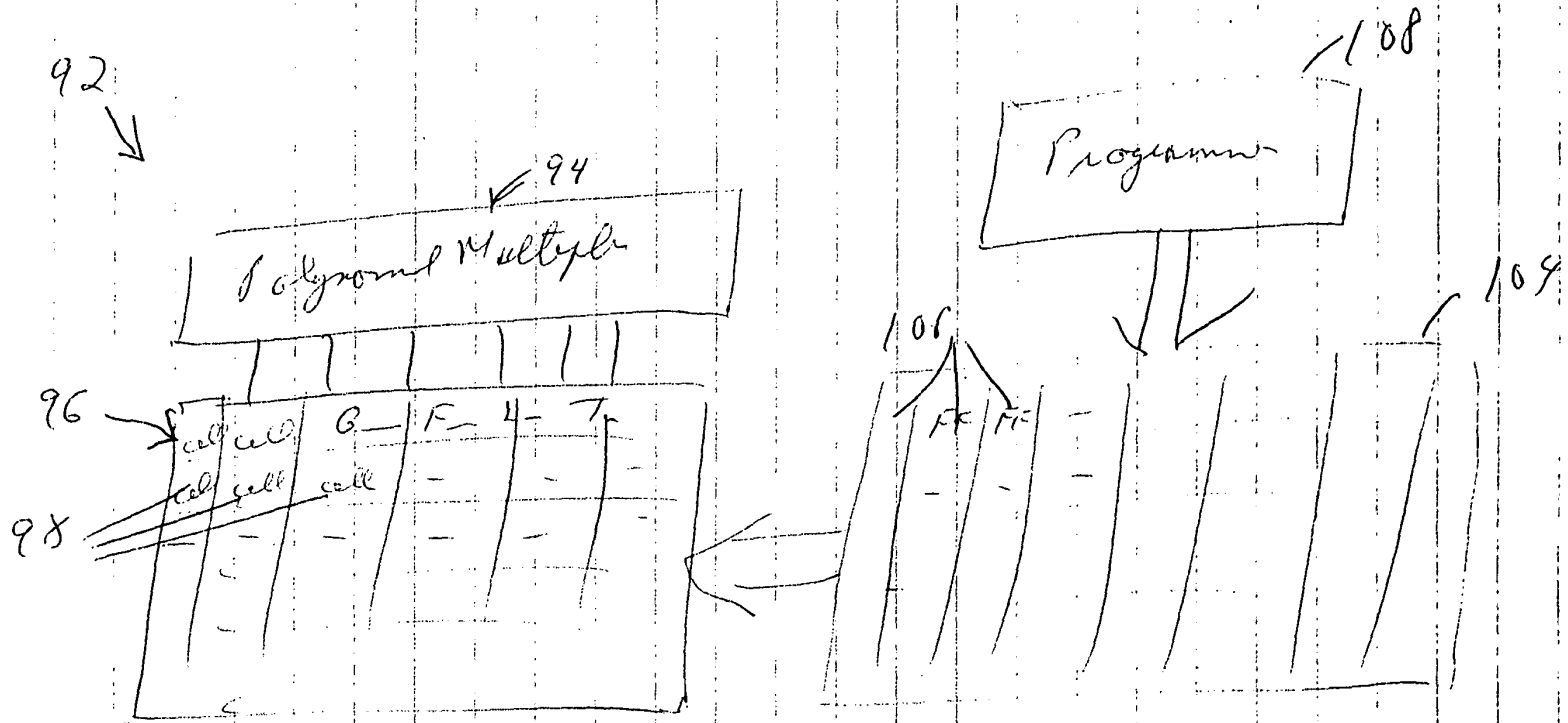

92
94
Polynomial Multiplier
96
98
108
Programmer
106
104

Fig. 7

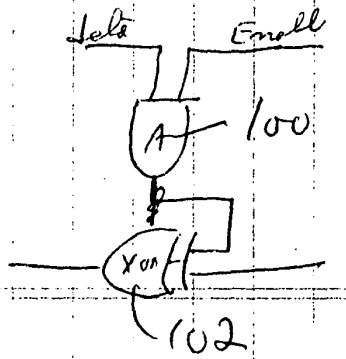

Data
Enable
98
A
100
Xor
102

Fig. 8

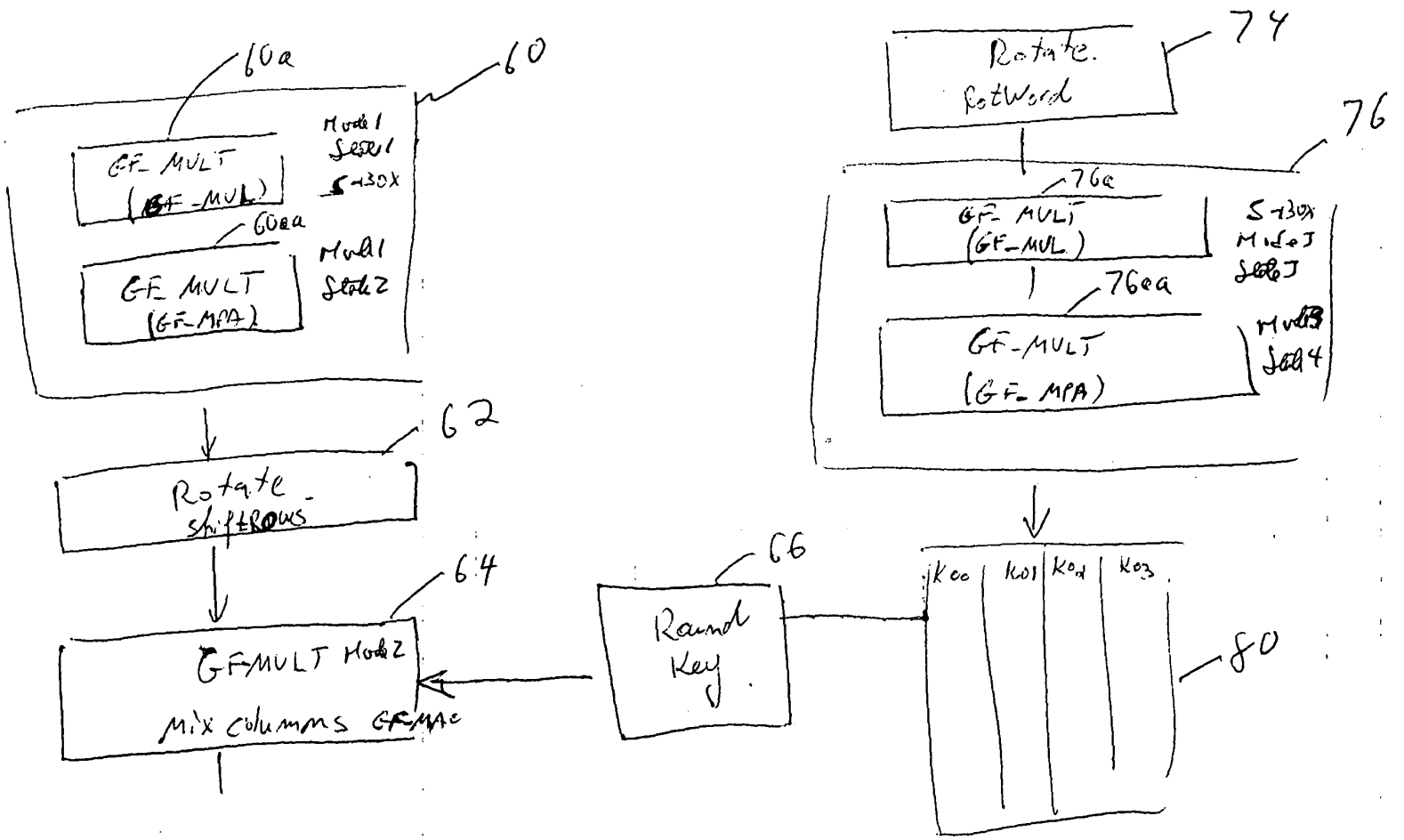
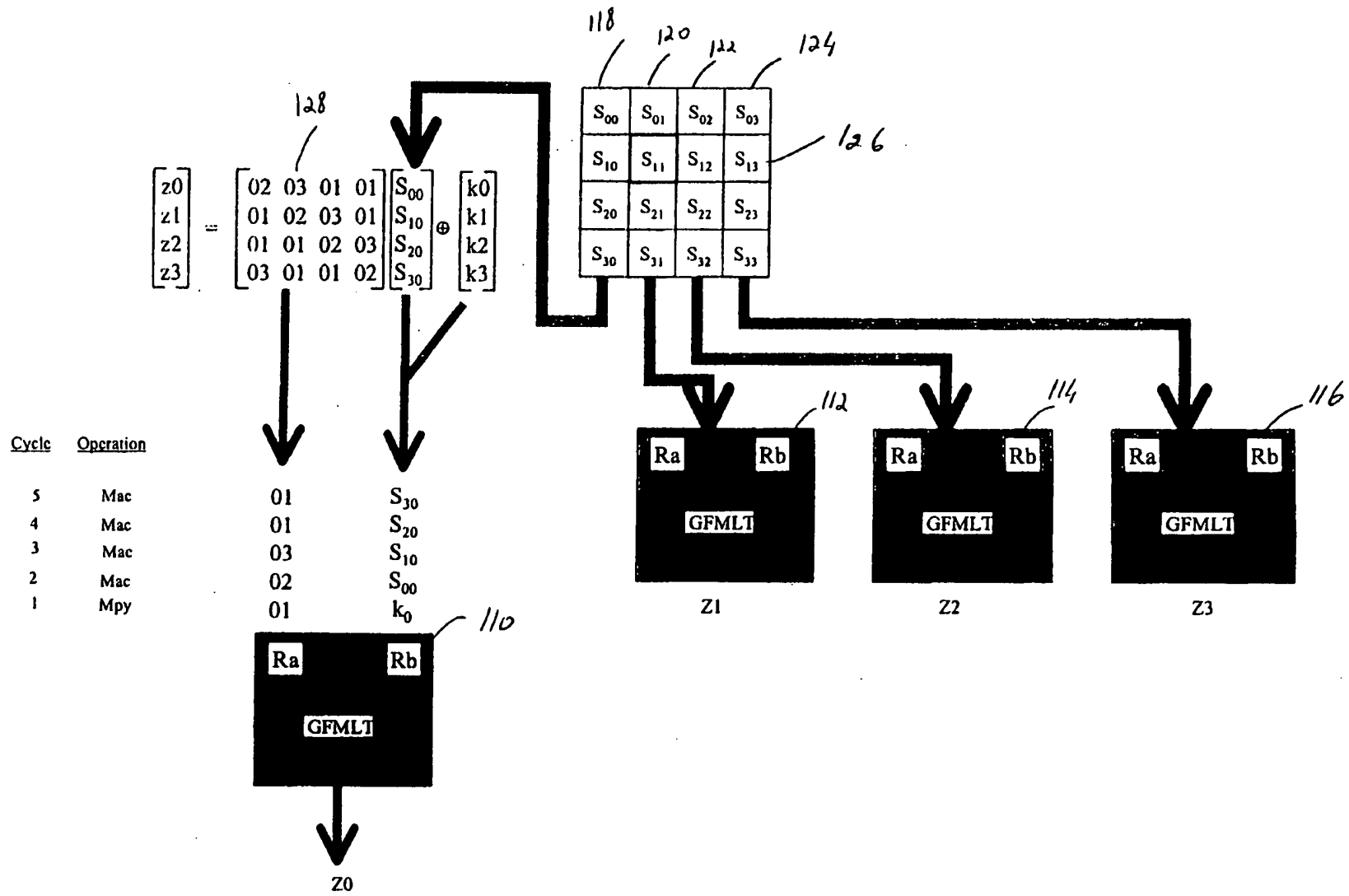

60a
60
GF_MULT (GF-MUL)
Mod1 Sel01 S-130x
60aa
GF_MULT (GF-MPA)
Mod1 Sel02
62
Rotate shiftRows
64
GF-MULT Mod2
Mix columns GF-MPc
66
Round Key
74
Rotate RotWord
76
76a
GF_MULT (GF-MUL)
S-130x Mod3 Sel3
76aa
GF-MULT (GF-MPA)
Mod3 Sel4
K00
K01
K02
K03
80

FIG. 9



$$Z_0 = (((((01 \otimes k_0) \oplus 02 \otimes S_{00}) \oplus 03 \otimes S_{10}) \oplus 01 \otimes S_{20}) \oplus 01 \otimes S_{30})$$

FIG. 10

GF_Mpy(β, α)

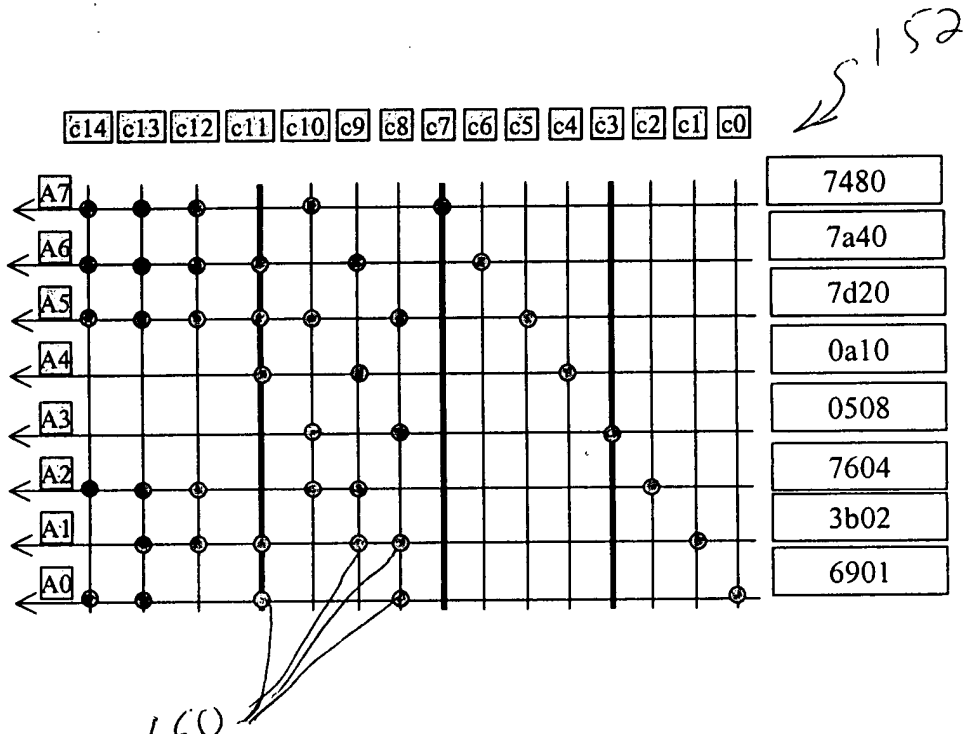
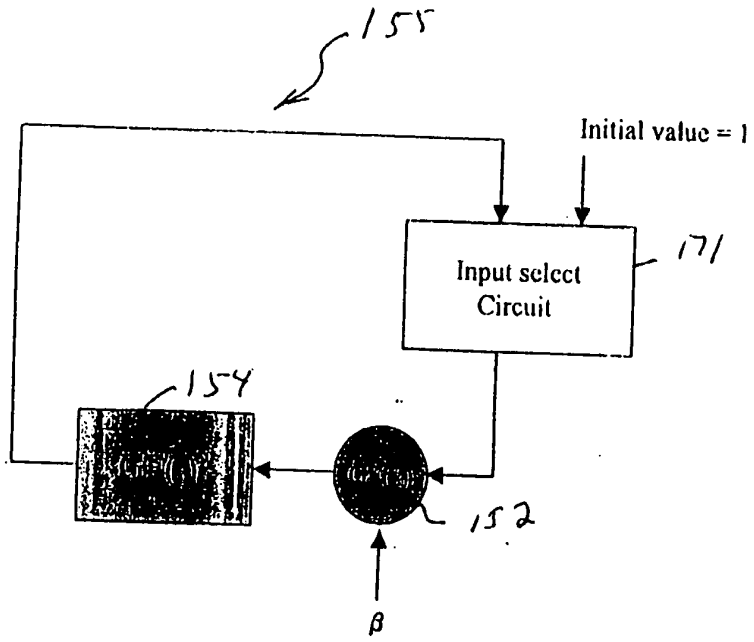


FIG. 11



$\beta^{q-1} = 1$ $\quad 1 : \beta$

$\beta^{q-2} = 1/\beta$ $\quad 1 q = 2^m$

$\beta^{2m-2} = 1/\beta$

Fig. 12

[illegible]

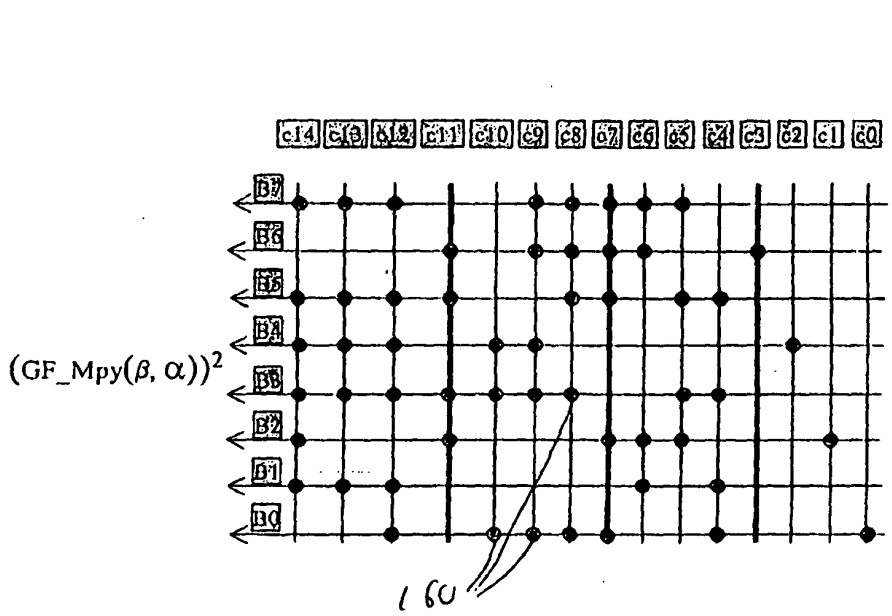

170
c14 c13 c12 c11 c10 c9 c8 c7 c6 c5 c4 c3 c2 c1 c0
B7
B6
B5
B4
B3
B2
B1
B0
$(GF\_Mpy(\beta, \alpha))^2$
160

FIG. 13

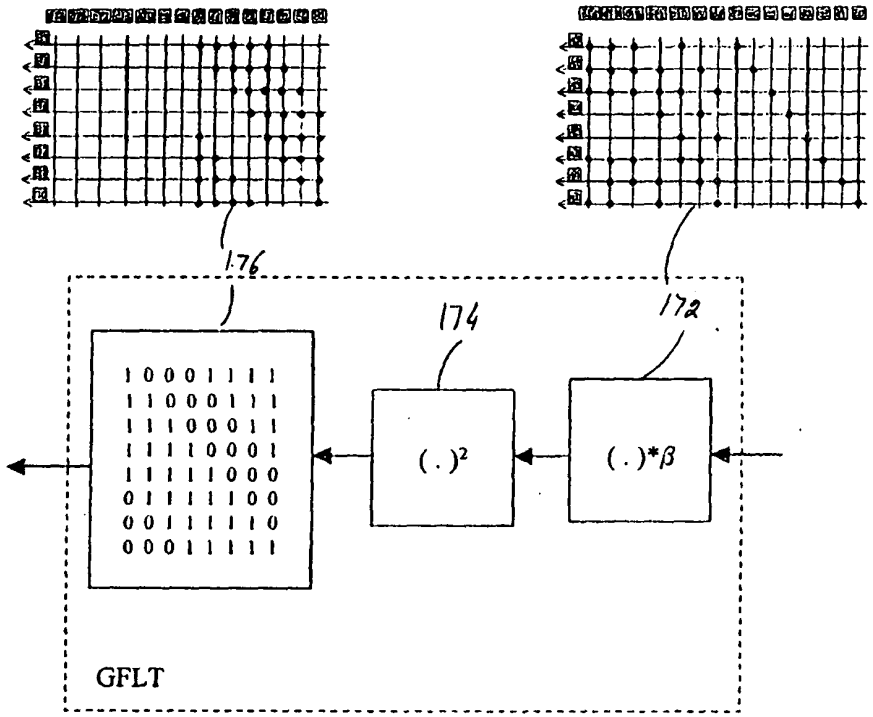

176
174
172
1 0 0 0 1 1 1 1
1 1 0 0 0 1 1 1
1 1 1 0 0 0 1 1
1 1 1 1 0 0 0 1
1 1 1 1 1 0 0 0
0 1 1 1 1 1 0 0
0 0 1 1 1 1 1 0
0 0 0 1 1 1 1 1
(.)²
(.)*β
GFLT

FIG. 14

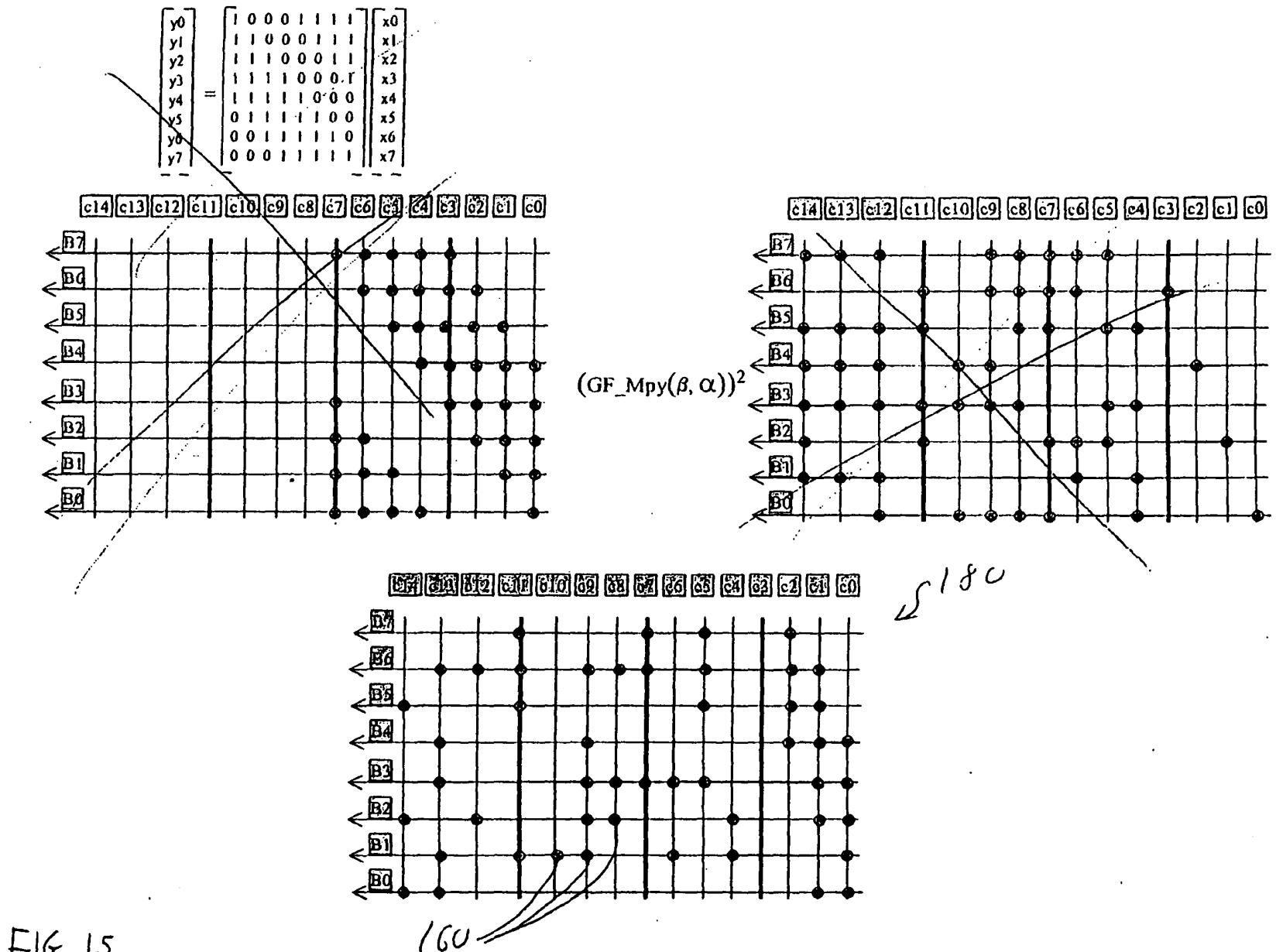
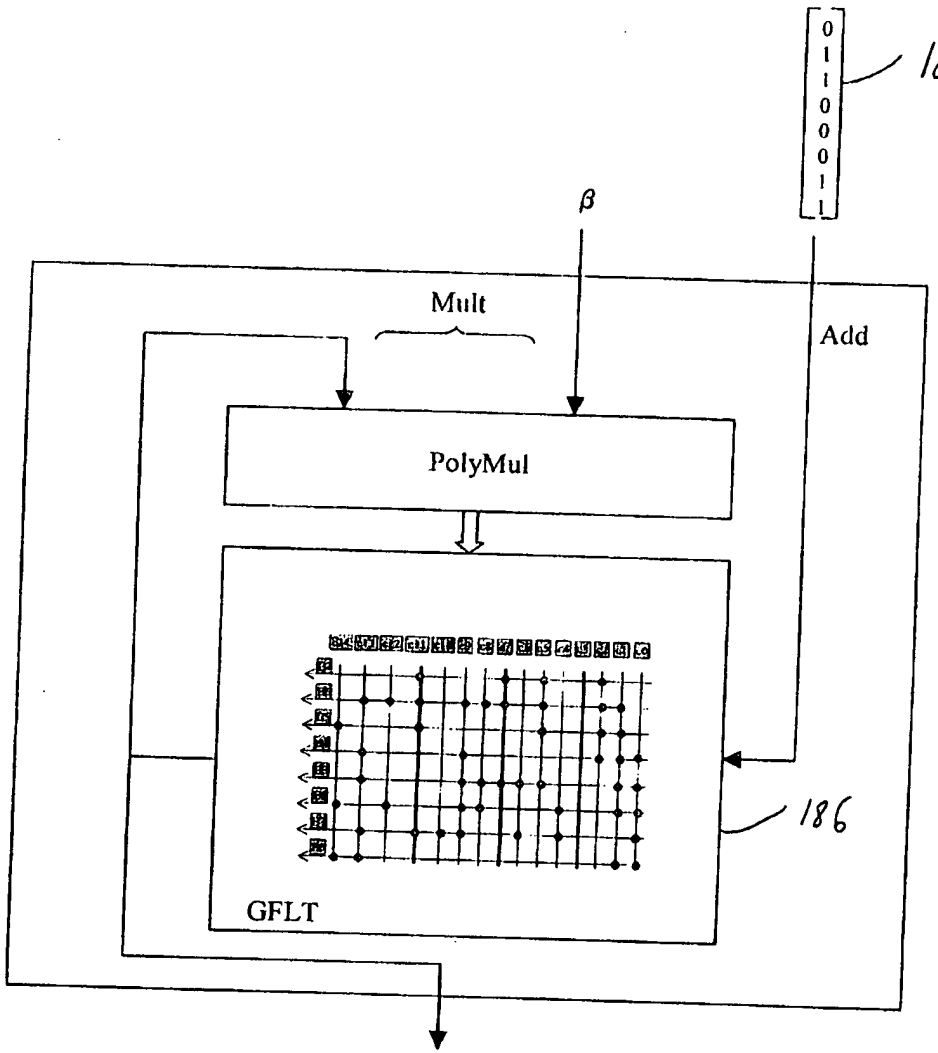

y0 y1 y2 y3 y4 y5 y6 y7 = x0 x1 x2 x3 x4 x5 x6 x7
c14 c13 c12 c11 c10 c9 c8 c7 c6 c5 c4 c3 c2 c1 c0
B7 B6 B5 B4 B3 B2 B1 B0
(GF_Mpy(β, α))²
180
160

FIG. 15



$$GF\_Out_n = Affine\_Transform\{[GF\_Mpy(GF\_Out_{n-1} * \beta)]^2\}$$

FIG. 16

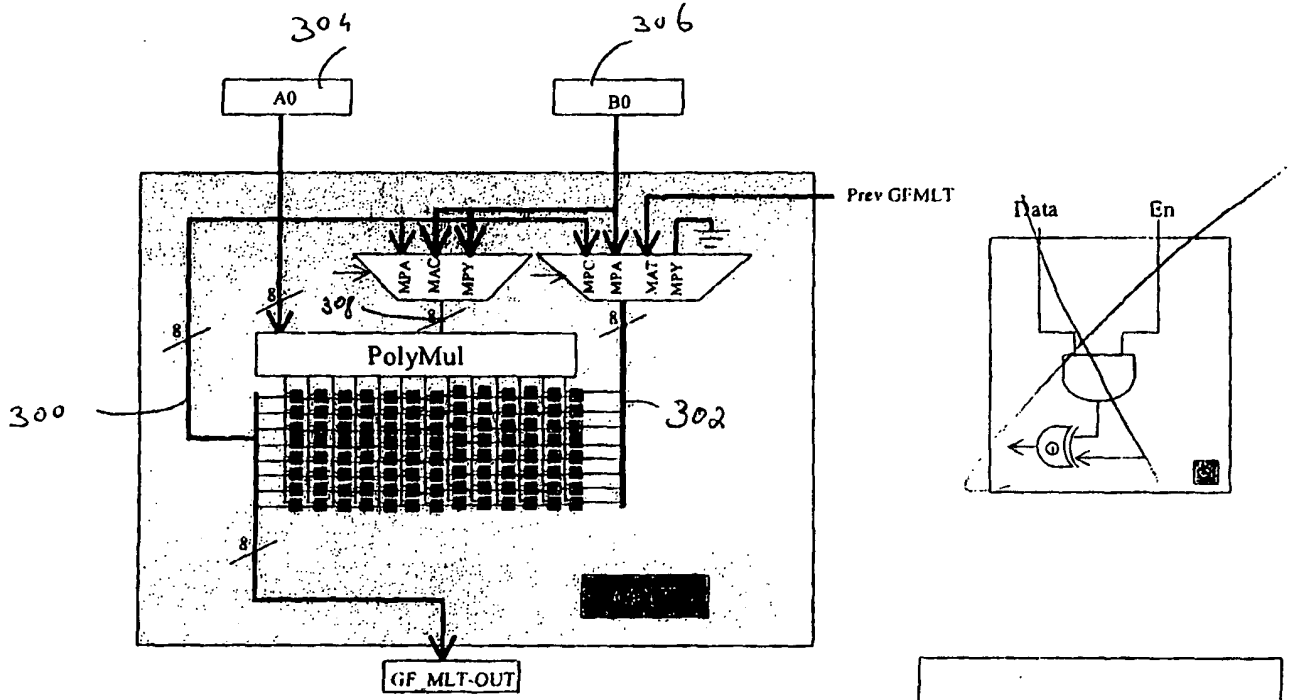

304
306
A0
B0
Prev GFMLT
MPA
MAC
MPY
MPC
MPA
MAT
MPY
8
308
PolyMul
300
302
GF_MLT-OUT
Data
En
Mpy = GF_MPY(A,B)
MPA = GF_MPY(GF$_{n-1}$,A) ⊕ B
MAC= GF_MPY(A*B) ⊕ GF$_{n-1}$
DIV = GFY(GF$_{n-1}$,A)

FIG. 17

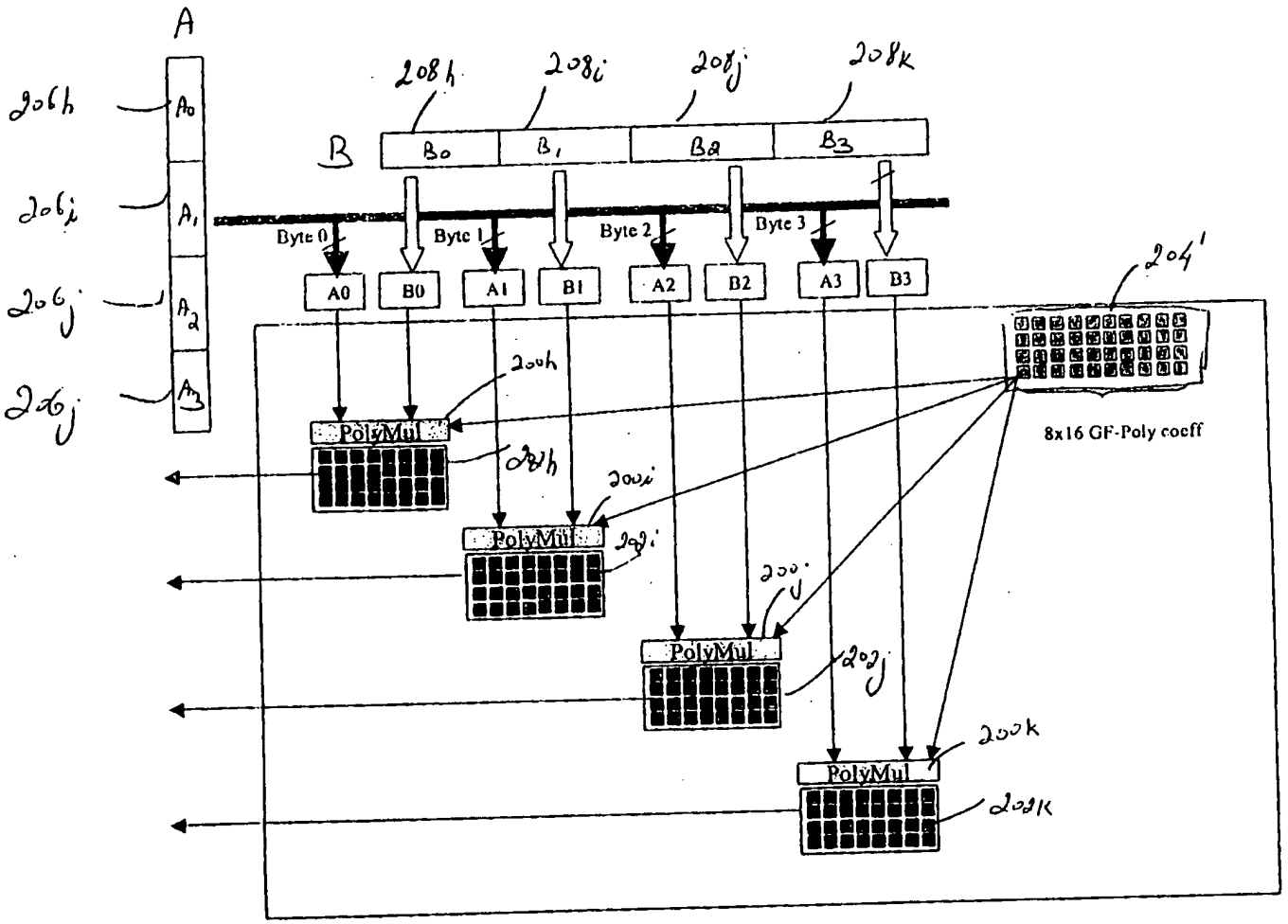

A
B
Byte 0
Byte 1
Byte 2
Byte 3
A0
B0
A1
B1
A2
B2
A3
B3
PolyMul
PolyMul
PolyMul
PolyMul
8x16 GF-Poly coeff

FIG. 18